How Many CAs are Enough?

Dr. Stephen Kent
Chief Scientist- Information Security
BBN Technologies

INTERNETWORKING
POWERED BY BBN

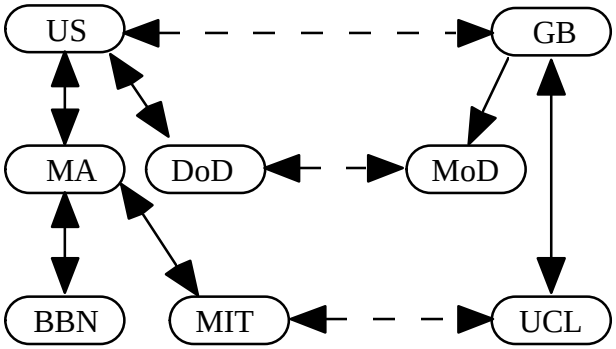
Outline

- Traditional certification models
- What makes for a good CA?
- Types of CAs
- Certificate mamagement issues
- The Mao Zedong model
- Conclusions

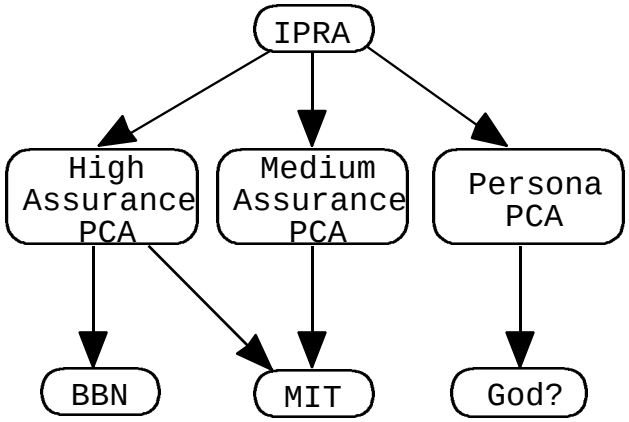
Traditional Certification Models

- X.509 (v1)
  - distinguished names are good for you
- PEM (RFC 1422)
  - yes, DNs are good
  - I think that I shall never see a certification graph lovelier than a tree
- PGP
  - we don’t need no stinkin’ DNs,we’ve got e-mail addresses
  - what do you mean one tree? everybody owns a forest!
- X.509 (v3)
  - a committee designed this standard (can’t you tell?)
  - any name is OK with us (though we still like DNs best)

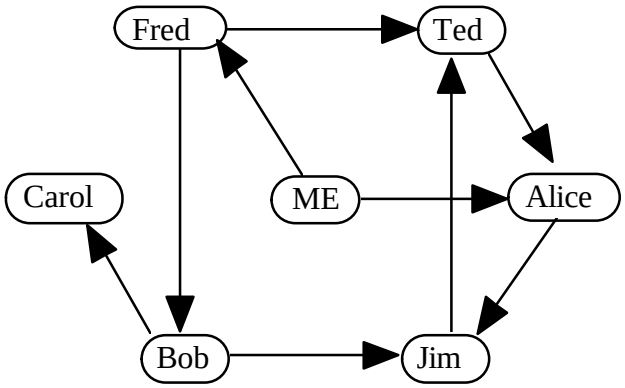
Certification Graphs



X.509



PEM

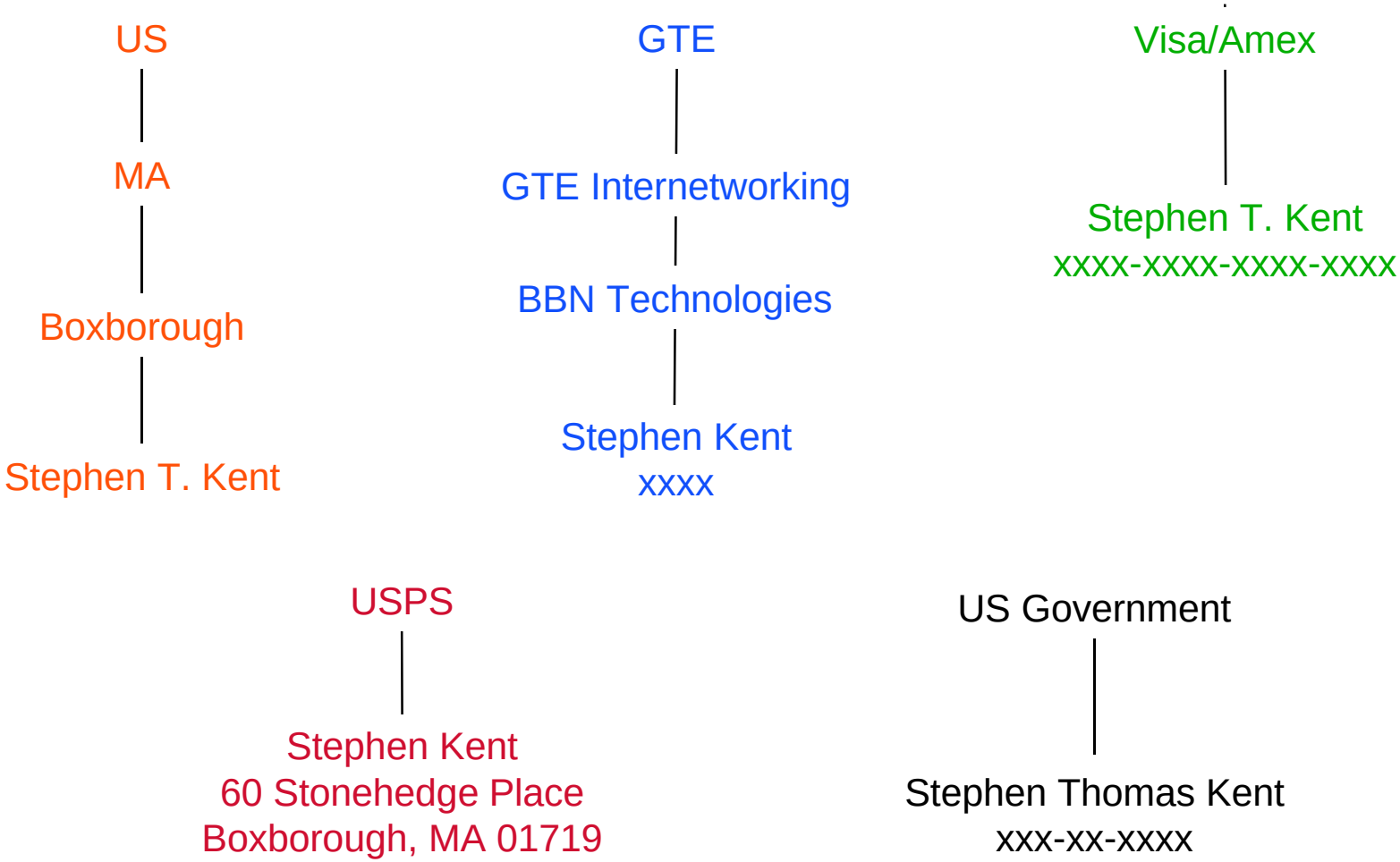


PGP

What Makes for a Good CA?

- Primary requirement:
  accurate binding of attributes to a public key
- Attribute types: identity, authorization, management
- Is the CA authoritative for the name space, or is this a matter of trust?
- Steve's Rule of Revocation: "The effective lifetime of a certificate is inversely proportional to the square of the number of attributes."

Example Name Spaces



Types of CAs

- Organizationally-empowered
  - *what's good for GM is good for CAs*
- Geopolitically-empowered
  - *I'm from the government and I'm here to certify you*
  - *I'm from a quasi-governmental agency and ...*
- Universally-empowered
  - *the Alexander Haig approach*
- Liability-empowered (third party)
  - *trust me, I'm a lawyer*
- Proprietary
  - *it's my name space and I'll certify if I want to*

What's Trust Got to do With It?

- Trust is a complex notion
  - trust is not transitive
  - trust is relative
  - trust is not quantifiable
- If a CA is authoritative for a name space, the elusive notion of *trust* is irrelevant
- One does not ask if Company X is *trusted* to identify its employees, or if the U.S State Department is *trusted* to identify U.S. Citizens, ...
- People cannot manage trust-based certification systems as the systems grow in size

Trusted vs. Authorized CAs

- No CAs are universally authorized or universally trusted!
- Authorized CAs
  - organizations (employees, clients, members, ...)
  - governments (citizens, residents, ...)
- Trusted CAs
  - third parties (anyone who pays)

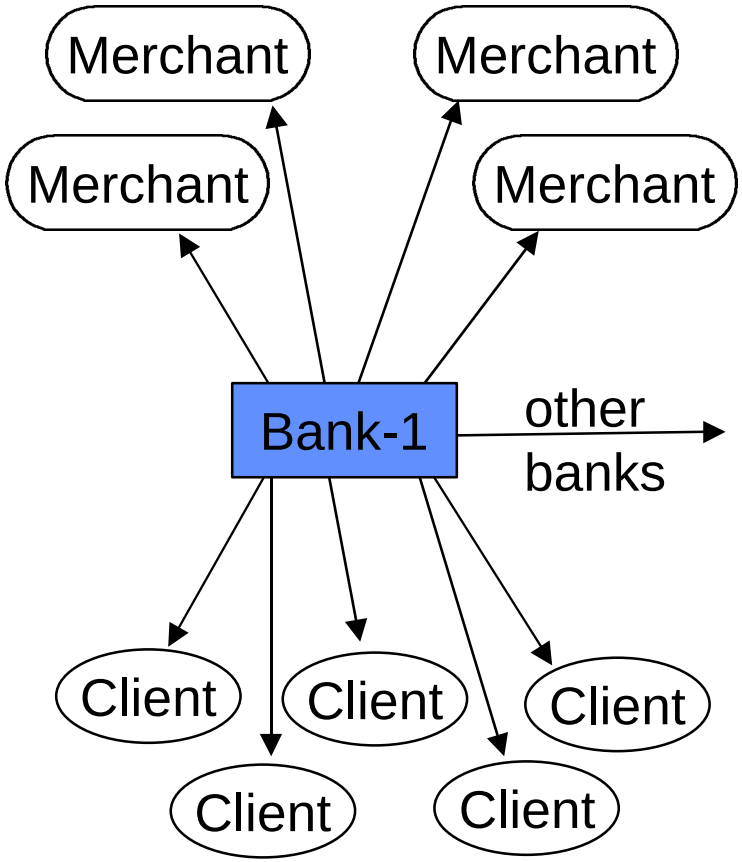
Certification Management Issues

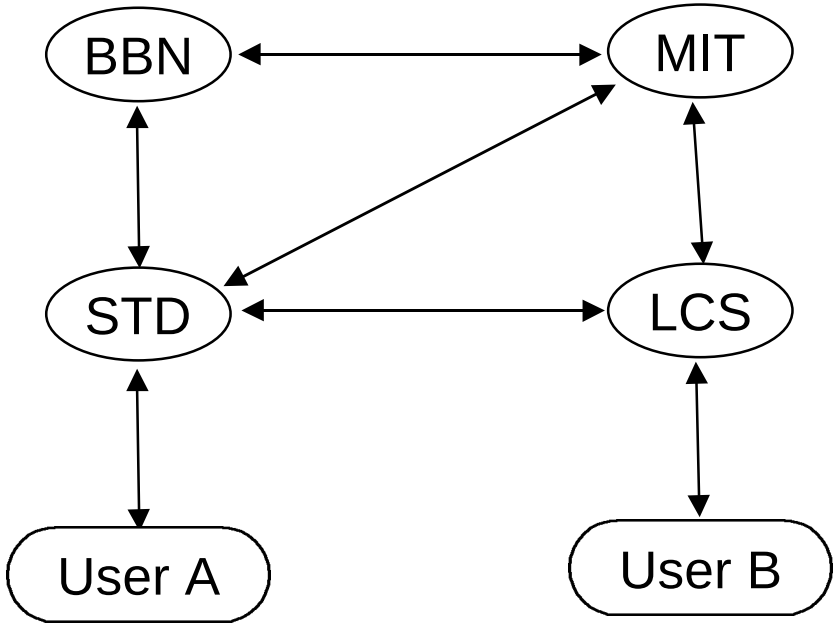
- Graph complexity
- Policy complexity
- Authorization data
- Non-verified data
- Revocation

Local Management Issues

- X.509 v3 certificates provide syntax for controlling certificate path validation algorithm
- But, mesh certification still entails management complexity in validation rule sets
- Human evaluation of certification paths is problematic
- Management errors create system vulnerabilities
- Remember VCRPlus® !

Two Certification Path Examples





Certification Policies

- Use as input to access control algorithms
- Used to specify:
  - security characteristics of the certification process
  - revocation procedures
  - security for user keying material
  - user authorization info?
- Binding policy info to certificates
  - simple identifiers
  - machine parsable syntax
  - pointers
  - included text

Policy Reference Examples

URL http://www.foo.bar.com/policy/ca

OID 2.16.840.1.101.2.1.3.1 (DMS)

TEXT The issuer of this certificate certifies only that the named subject presented one or more valid forms of picture identification (including but not limited to a driver's license issued by one of the states, possessions , or protectorates of the United States of America, a passport or permanent alien registration card issued by the U.S State Department, or a college yearbook from an accredited four (4) year college or university within the United States) in the presence of a registered notary public in the state of Utah, and that the issuer paid some scant attention to the subject name form and the identification presented by the alleged subject. The certificate issuer shall not be held liable for any consequential damages that might result from actual use of this certificate in any form of electronic commerce, except to the extent that state laws prohibit waiver of such liability by a CA attempting to make a quick buck while remaining totally blameless, etc., etc., etc.

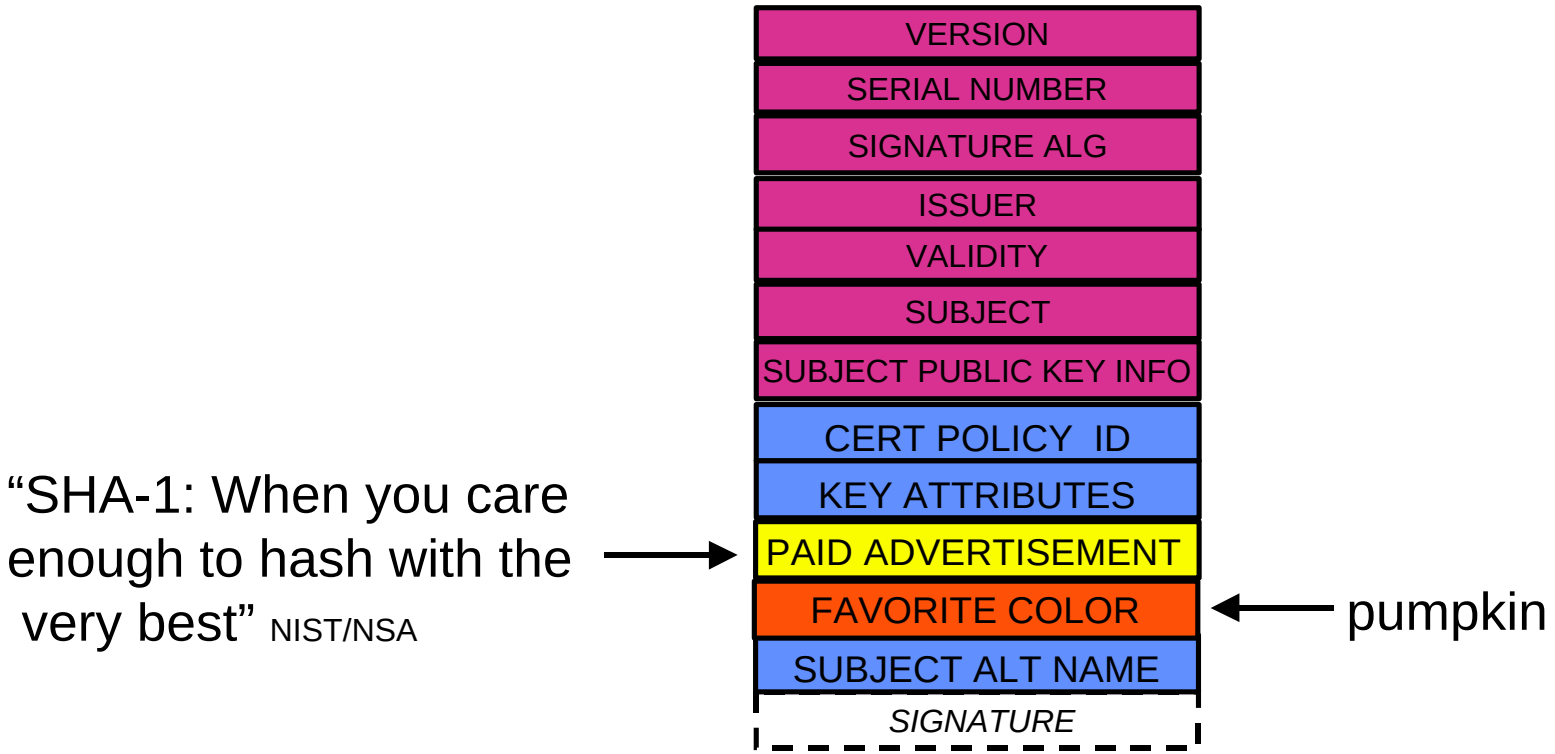
Authorization Data in Certificates

- Concept
  - add authorization data to identification data in a certificate
- Motivation
  - certificates are a convenient way to transport data with integrity
- Mechanism
  - define new extensions, mark as critical when appropriate
- Problem
  - authority scope conflicts, inconsistent validity intervals, ...
- Steve's Rule of Revocation
  - "The effective lifetime of a certificate is proportional to the inverse of the square of the number of attributes in the certificate."

“Non-Verified” Information

- Concept
  - include data in a certificate that the CA has not “verified”
- Motivation
  - certificates are a convenient way to transport data with integrity, bound to the subject ID and other cert contents
- Mechanism
  - add another flag to indicate the data is not verified, so that the CA absolved of liability
- Question
  - if it’s not verified, why bother?

Certificate with NVI



Revocation

- CRLs are the canonical certificate revocation model
- But CRLs are slow, based on a periodic pull model
- Pushing CRLs is hard, since one doesn’t know to whom CRLs are relevant
- Online validation is an alternative, and use of a separate CA key for that purpose reduces risks associated with the online access to this function
- But procedural aspects of revocation may be the limiting factor in timely notice of revocation
- ACLs are an alternative to revocation for use access control systems

Problems of Third Party CAs

- Cost- can you charge enough for certification as an independent business activity, without charging too much?
- Assurance- what are the right levels of assurance for a wide range of applications?
- Naming- what is the “right” name form for many different applications? can one CA be authoritative for many different name forms?
- Liability- what is the right tradeoff between assuming responsibility as a CA and not assuming unlimited liability?

Mao Zedong Certification Model

- Lots of CAs (“let 10,000 flowers bloom”)
- Organizational and proprietary CAs
- Each proprietary CA serves an application or a group of related applications
- The certificate subject name is a combination of a common name and an account number, usually tied to an existing database
- Servers ask for the right client certificate (alà SSL 3.0)
- Organizations can issue certificates on-line, via query/response conversation, protected via SSL, maybe with out-of-band confirmation

Advantages of the Mao Model

- CAs are authoritative for name spaces
- No complex trust models required
- Easy certificate validation and revocation
- Liability limited to the application context
- Very low costs
- Assurance appropriate to the application context
- Clear policy scope

A Role for Third Party CAs?

- Need to avoid $O(n^2)$ cross-certification problem, for communication among many organizations
- Certificate acquisition problem for proprietary CAs
- Governments (federal, state, or local) are appropriate "top level" CAs for certifying organizations of all sorts
- CA operations can be outsourced, with government agencies acting as RAs
- Thus there is an appropriate role for "public" CAs, as service providers for organizations, governments, etc.

Conclusions

- We still have a lot to learn about good CA practices
- Near term PKI trends
  - proprietary PKIs for financial applications
  - organizational PKIs for intranet use
  - liability-empowered (third party) PKIs for ?
- Geopolitical PKIs will take longer but hold promise, and are essential for scaling
- Keep certificates and certificate management simple
  - don’t overload certificates withextraneous attributes
  - don’t create complex validation policies
  - do use cross certification with name constraints